UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,979	08/31/2000	Adrian Shields	8490.00	3073

26889 7590 12/23/2008

MICHAEL CHAN
NCR CORPORATION
1700 SOUTH PATTERSON BLVD
DAYTON, OH 45479-0001

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
12/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ADRIAN SHIELDS

Appeal 2008-4271
Application 09/651,979[1]
Technology Center 2400

Decided: December 22, 2008

Before LANCE LEONARD BARRY, JEAN R. HOMERE, and JAY P. LUCAS, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellant appeals under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 21 through 38. Claims 1 through 20 have been canceled. We have jurisdiction under 35 U.S.C. § 6(b). We affirm-in-part.

---

[1] Filed on August 31, 2000. The real party in interest is NCR Corp.

The Invention

As shown in Figure 4, Appellant invented a method and apparatus (50) for securely exchanging transaction information between in a portable terminal (PDA, 10) and a financial institution (ATM 52). (Spec. 1.) As depicted in Figures 1-2, the portable terminal may be a personal digital assistant (PDA) (10), which includes a storage area (28) that contains financial account data (30) for a financial institution, an ATM program (32) for preparing ATM transactions, and an encryption program (34) for encrypting the prepared ATM transactions. (Spec. 7.) Upon a user starting a new session for performing a financial transaction on the PDA (10), the encryption program (34) obtains a seed from stored records and hashes it to thereby generate a new session key for the transaction. (Spec. 8.) The PDA (10) then uses a public key stored in the account data (30) to encrypt the new session key, which is transmitted to the automated teller machine (ATM) (52). (Spec. 9.) The PDA (10) subsequently uses the session key to decrypt an encrypted response received from the ATM (52). (*Id.*)

Illustrative Claim

Independent claim 21 further illustrates the invention. It reads as follows:

21. A method of operating a portable computer, comprising:

a) storing records of events experienced by the computer in user-accessible memory within the computer;

b) using one or more of the records as seed for generating plain text of a first session key KI; and then

c) encrypting KI, transmitting Kl (encrypted) to an external terminal, receiving an encrypted response from the external terminal, and de-crypting the encrypted response using the plain text of KI.

Prior Art Relied Upon

The Examiner relies on the following prior art as evidence of unpatentability:

Yacobi	US 5,878,138	Mar. 2, 1999
Kawan	US 2002/0062284 A1	May 23, 2002 (filed Jan. 28, 1999)

Alfred J. Menezes et al., *Handbook of Applied Crytography,* CRC Press, pp. 170-172, 494, and 552 (1997).

Rejections on Appeal

The Examiner rejects the claims on appeal as follows:

A. Claims 21 through 34 and 38 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Yacobi and Menezes.

B. Claims 35 through 37 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Yacobi, Menezes, and Kawan.

Appellant's Contentions

Appellant argues that the combination of Yacobi and Menezes does not render claims 21 through 34 and 38 unpatentable. (App. Br. 25-70, Reply Br. 1-28.) Particularly, Appellant argues that Yacobi does not teach or suggest decrypting on a portable computer an encrypted response using a first session key. (App. Br. 25-31, Reply Br. 1-3.) Appellant argues that while Yacobi discloses encrypting[2] digital cash returned to an electronic wallet, such encryption is not done using the generated session key. Further, Appellant argues that Yacobi does not teach that the electronic wallet decrypts the digital cash using the same generated session key. (Reply Br. 4-9.) Further, Appellant argues that there would be insufficient rationale to support the Examiner's suggested combination of Menezes' data seed with Yacobi's session key to encrypt and decrypt a response, as recited in independent claim 21. (App. Br. 40-47, Reply Br. 11-18.)

Examiner's Findings/Conclusions

The Examiner finds that Yacobi's disclosure of using the session key to establish a secure channel through which the bank transmits to the electronic wallet digital coin encrypted with its private key fairly teaches or

[2] Appellant previously argued, at pages 25-27, 32-39 of the Appeal Brief, that Yacobi's disclosure of the bank hashing the digital cash does not teach or suggest an encrypted response. However, in the Reply Brief, Appellant appears to have acknowledged that Yacobi's hashing of the digital cash in conjunction with the issued digital certificates constitutes an encrypted response. (Reply Br. 4.)

suggests a portable computer that receives an encrypted response from an external terminal using a session key, as recited in independent claim 21. (Ans. 6-8.) Similarly, the Examiner finds that Yacobi's disclosure of the electronic wallet using the plain value of the received encrypted digital coin at a merchant suggests that the digital coin must have been decrypted. (*Id.*) Additionally, the Examiner finds that one of ordinary skill in the art would have known how to generate Yacobi's session key from Menezes' seed. (Ans. 9-12.) Therefore, the Examiner concludes that the combination of Yacobi and Menezes renders claim 21 unpatentable. (*Id.*)

II. ISSUE

The pivotal issue before us is whether Appellant has shown that the Examiner erred in concluding that the combination of Yacobi and Menezes renders the claimed invention unpatentable. Particularly, the issue turns on whether the ordinarily skilled artisan would have found sufficient rationale to combine the cited references to teach (1) encrypting a generated session key using a public key before transferring the encrypted key to an external computer, and (2) decrypting an encrypted response using the session key, as recited in independent claim 21.

III. FINDINGS OF FACT

The following findings of fact (FF) are supported by a preponderance of the evidence.

Yacobi

1. Yacobi discloses an electronic asset system for allowing an electronic wallet and a bank's computer to securely perform financial transactions. As depicted in Figure 2, the electronic wallet (58) is a portable computer manufactured with initial pairs of public and private keys, and a corresponding certificate registered with the bank's computer. The electronic wallet has a processor, a program memory, a volatile memory, and a non-volatile memory. (Col. 8, ll. 39-45, ll. 50-53.)

2. The electronic wallet (58) has a cryptographic program in memory that directs the processor to encrypt/decrypt data, to generate a unique pair of cryptographic keys that are transmitted to the bank's computer (62) along with the user's identification. The bank's computer uses the transmitted pair of digital keys in conjunction with the registered certificate to create an initial secure communication channel, which is used to authenticate the digital wallet and the bank's computer. (Col. 9, ll. 1-9.)

3. Upon completing the initial verification process, the user's wallet (58) generates a session key, which it uses to encrypt a message being transferred to the bank's computer. The wallet subsequently encrypts the generated session key using the public exchange key of the bank's computer previously received in the bank's certificate. Further, the wallet uses its own private key to sign the encrypted message, which it transfers along with the encrypted session key to the bank's computer via the secure channel. (Col. 9, ll. 44-54.)

4. Upon receiving the encrypted session key and the signed encrypted message, the bank's computer uses its own private exchange key to decrypt the session key. Then, the bank's computer uses the decrypted session key to decrypt the signed encrypted message. Individual keys that are used for each secure messaging and transmission are subsequently destroyed. (Col. 9, ll. 54-57, col. 9, l. 65- col. 10, l. 1.)

5. Upon receiving a request from a user's electronic wallet (58) to obtain digital cash, the bank's computer (62) generates a response message including the requested digital cash, and a data string. It hashes the data string, and uses its own private signing key to sign the hashed data string. Additionally, the bank's computer employs a different pair of signing keys for each digital coin denomination. (Col. 10, ll. 17-31.)

6. Once the generated digital coins (70) are downloaded in the electronic wallet over the secure communication channel (68), they are stored in the wallet for later use. If the user wishes to purchase services or items from a merchant (56), after establishing a secure communication channel (72) with the merchant (56), the user digitally signs the coins contained before tendering them to the merchant (56). (Col. 10, ll. 32-48.)

7. Periodically, the merchant's computer (76) establishes a secure communication channel to deposit the received signed coins with the bank's computer (62). (Col. 10, ll. 57-65.)

Menezes

8. Menezes discloses a software-based random bit generator that produces random bits based on a plurality of factors including user input, system clock, contents of input/output buffer, operating system, and elapsed time between keystrokes. (P. 172.)

Kawan

9. Kawan discloses a user entering a PIN into a PDA before the user can be allowed to perform or complete a transaction. (P. 3, para. [0030].)

IV. PRINCIPLES OF LAW

Claim Construction

"[T]he words of a claim 'are generally given their ordinary and customary meaning.'" *Phillips v. AWH Corp.,* 415 F.3d 1303, 1312 (internal citations omitted). "[T]he ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Id.* at 1313.

"[T]he PTO gives claims their 'broadest reasonable interpretation.'" *In re Bigio*, 381 F.3d 1320, 1324 (Fed. Cir. 2004) (quoting *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000)). "Moreover, limitations are not to be read into the claims from the specification." *In re Van Geuns*, 988 F.2d 1181,

1184 (Fed. Cir. 1993) (citing *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989)). Our reviewing court has repeatedly warned against confining the claims to specific embodiments described in the specification. *Phillips v. AWH Corp.*, 415 F.3d at 1323.

Obviousness

Appellant has the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

> Section 103 forbids issuance of a patent when "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains."

KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727, 1734 (2007).

In *KSR*, the Supreme Court emphasized "the need for caution in granting a patent based on the combination of elements found in the prior art," and discussed circumstances in which a patent might be determined to be obvious. *KSR,* 127 S. Ct. at 1739 (citing *Graham v. John Deere Co.*, 383 U.S. 1, 12 (1966)). The Court reaffirmed principles based on its precedent

that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id.* The operative question in this "functional approach" is thus "whether the improvement is more than the predictable use of prior art elements according to their established functions." *Id.* at 1740.

The Federal Circuit recently recognized that "[a]n obviousness determination is not the result of a rigid formula disassociated from the consideration of the facts of a case. Indeed, the common sense of those skilled in the art demonstrates why some combinations would have been obvious where others would not." *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1161 (Fed. Cir. 2007) (citing *KSR*, 127 S. Ct. 1727, 1739 (2007)). The Federal Circuit relied in part on the fact that Leapfrog had presented no evidence that the inclusion of a reader in the combined device was "uniquely challenging or difficult for one of ordinary skill in the art" or "represented an unobvious step over the prior art." *Id.* at 1162 (citing *KSR*, 127 S. Ct. at 1740-41).

One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. *In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986).

The test for obviousness is what the combined teachings of the references would have suggested to one of ordinary skill in the art. *See In re Kahn*, 441 F.3d 977, 987-988 (Fed. Cir. 2006), *In re Young*, 927 F.2d 588, 591 (Fed. Cir. 1991) and *In re Keller*, 642 F.2d 413, 425 (CCPA 1981).

Moreover, in evaluating such references it is proper to take into account not only the specific teachings of the references but also the inferences which one skilled in the art would reasonably be expected to draw therefrom. *In re Preda*, 401 F.2d 825, 826 (CCPA 1968).

V. ANALYSIS

35 U.S.C. § 103

Claims 21-23, 35, and 38

Independent claim 21 recites in relevant part decrypting on a portable computer an encrypted response using a generated session key. As detailed in the Findings of Facts section, Yacobi discloses that the bank uses its own private key to digitally sign a hash value to thereby create digital coins that are downloaded into the user's electronic wallet via a secure communication channel. (FF. 5-6.) Yacobi further discloses that the user can purchase goods or services from a merchant by signing the digital coins and downloading them into the merchant's computer via a secure channel. (FF. 7.) The ordinarily skilled artisan would recognize that the generated digital coins that the user's electronic wallet receives from the bank are not encrypted, and need not be decrypted thereafter upon receipt. While it is reasonable to find that Yacobi's bank response to the user's request utilizes digitally signed cryptographic data to generate the digital coins, the ordinarily skilled artisan would appreciate that the ensuing digital coins downloaded into the electronic wallet are not encrypted. Therefore, we find

no need in Yacobi's system for decrypting the received digital coins on the electronic wallet. Thus, we agree with Appellant that Yacobi does not teach or suggest the decryption of an encrypted response using a generated session key. Further, we find that Menezes does not cure the deficiencies of Yacobi. It follows that Appellant has shown that the Examiner erred in concluding that the combination of Yacobi and Menezes renders claim 21 unpatentable.

Since claims 22, 23, 35, and 38 recites the same disputed limitation, we conclude for the reasons outlined above that Appellant has shown error in the Examiner's conclusion that the cited claims are unpatentable over the suggested combination. Therefore, we will not sustain the Examiner's rejection of claims 21 through 23, 35, and 38.

Claims 24-34, and 36-37

As to claim 24, Appellant argues that the combination of Yacobi and Menezes does not teach encrypting two session keys using a public key, and transmitting the encrypted keys to an external device. (App. Br. 48-49). We do not agree. As detailed in the Findings of Fact section, Yacobi discloses that the electronic wallet uses a public exchange key received from the bank's computer to encrypt a generated session key, and subsequently transfers the encrypted key to the bank. (FF. 3.) Further, Yacobi teaches each key used for communication or transmission is subsequently destroyed. (FF. 4.) The ordinarily skilled artisan would readily appreciate from Yacobi's teachings that for each new session, a new session key is

generated, encrypted with the public exchange key before being transmitted to the bank. Therefore, the combination of Yacobi and Menezes reasonably teaches or suggests that the electronic wallet generates a plurality of session keys that are encrypted with a public exchange key before being transmitted to the bank.

Appellant did not provide separate arguments with respect to the rejection of dependent claim 25. Consequently, claim 25 falls together with representative claim 24. 37 C.F.R. § 41.37(c)(1)(vii).

As to dependent claims 26, 27, 32, and 37, Appellant argues that the combination of Yacobi and Menzes does not teach or suggest decrypting on a portable computer an encrypted message using a generated session key. (App. Br. 49). We agree with Appellant for the reasons detailed above. We therefore, will not sustain the Examiner's rejection of these claims.

As to claims 28-29, Appellant argues that Yacobi teaches a tamper-resistant device, as opposed to the claimed "no-secure area" for storing an encryption key. (App. Br. 73.) We do not agree. As detailed in Findings of Fact section, Yacobi discloses a volatile memory region for storing an encryption key. (FF. 1.) The ordinarily skilled artisan would readily recognize that the volatile memory is a non-secure area of memory. Therefore, the combination of Yacobi and Menezes reasonably teaches or suggests the limitations of the cited claims.

As to claims 33 and 36, Appellant argues that there is insufficient rationale for combining Yacobi with Menezes and/Kawan to arrive to the

claimed invention. (App. Br. 52-70.) We do not agree. The ordinarily skilled artisan would appreciate that Yacobi, Menezes, and Kawan disclose prior art elements that perform their ordinary functions to predictably result in a portable computer wherein a user first enters a PIN to generate a seed to thereby create a session key before the user can be allowed to perform or complete a financial transaction with an ATM. We therefore, do not agree with Appellant that there is insufficient rationale for combining cited references. Likewise, we do not agree with Appellant that Menezes teaches away from Yacobi. It follows that Appellant has not shown that the Examiner erred in concluding that the combination of Yacobi, Menezes, and/or Kawan renders the cited claims unpatentable.

VI. CONCLUSIONS OF LAW

A. Appellant has shown that the Examiner erred in concluding that the combination of:

   1. Yacobi and Menezes renders claims 21 through 23, 26, 27, 32, and 38 unpatentable under 35 U.S.C. § 103(a).

   2. Yacobi, Menezes, and Kawan renders claims 35 and 37 unpatentable under 35 U.S.C. § 103(a).

B. Appellant has not shown that the Examiner erred in concluding that the combination of:

   1. Yacobi and Menezes renders claims 24, 25, 28 through 31, 33, and 34 unpatentable under 35 U.S.C. § 103(a).

2. Yacobi, Menezes, and Kawan renders claim 36 unpatentable under 35 U.S.C. § 103(a).

VII. DECISION

We reverse the Examiner's decision to reject claims 21 through 23, 26, 27, 32, 35, 37, and 38. However, we affirm the Examiner's decision to reject claims 24, 25, 28 through 31, 33, 34, and 36.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

rwk

MICHAEL CHAN
NCR CORPORATION
1700 SOUTH PATTERSON BLVD
DAYTON OH 45479-0001